Functional Package for Systems Transmitting Sensitive HCFA data (STS-HCFA)
Guide for Reviewers

BACKGROUND

Why the Functional Package is being developed

The HCFA Internet Security Policy is a policy document that was issued by HCFA in November 1998 to stipulate security requirements for any information system used by HCFA stakeholders (including medicare/medicaid care providers, state agencies acting as HCFA agents etc.,) to transmit & receive HCFA sensitive data. As with any policy requirements this may be interpreted in many different ways by different system vendors and users. Using a common language to map these requirements to system-level security specifications/requirements will go a long way in promoting understanding of these policy provisions and promote better communications among the procurers of these systems and the vendors/consultants who promote the use and deployment of these systems.

The International Security Criteria standard (ISO/IEC 15408) and its frameworks provide such a common and flexible language infrastructure for expression of system security services/requirements both from the vendor and user perspective alike. One such framework is the "Functional Package" which provides a means for aggregating all the security requirements/services pertaining to a given federal policy or a set of policies and put them at the level of system-level requirements. Further the set of aggregated security requirements stated in a Functional Package can be readily be used a pre-defined module in other ISO/IEC 15408 frameworks like "Security Protection Profiles/Security Targets" . These frameworks are the ones that are ultimately used as the basis for evaluating information systems for compliance to mandated policy requirements.

Technical Approach

The HCFA Internet Security Policy has stipulated the use of certain types of technologies to guarantee certain minimum level of effectiveness with regard to the implementation of security safeguards for HCFA-sensitive information travelling over the public Internet. Since not all these technologies had universal standards like ISO & IETF to guide their implementations, some system level security service requirements have to be formulated based on de-facto standards like SSL V3.0 & S/MIME. Further in formulating system-level security service requirements, one has to take into account not only policy dictates (e.g., which in our case is the HCFA Internet Security Policy requirements) but also the dictates of the threat/risk assessment model that a particular organization may have developed over time. In our Functional Package (which is intended to cover all types of systems transmitting HCFA-sensitive data and being deployed in widely varying security environments), we had to assume a generic set of threats & vulnerabilities that any system interacting with the Internet had to counter. This Functional Package can therefore be fine tuned to take into account the specific threats identified in a specific organization's threat model.

Guidelines followed in development of this Functional Package : The Functional Package is a valid framework under the Common Criteria (the predecessor to ISO/IEC 15408) although the ISO/IEC 15408 itself is yet to formalize the guidelines for production of a Functional Package. The Functional Package is meant to be a framework for aggregating all the security service requirements pertaining to a given policy(ies) & organizational operating assumptions and intended to cover an entire family of systems that provides the functionality/business process that is covered by the policy. Therefore, the Functional Package is not meant for covering "system security specifications" for a given application system (but to a family of systems that support a business process) and hence it does not contain the "security assurance components" (since assurance components can only for useful for a given application system with clear boundaries & interfaces)). Hence the Functional Package can be viewed as a Security Protection Profile without the security assurance components. Hence the author followed the ISO Guide for Production of Protection Profiles and Security Targets, v 0.8 (7/99) while producing this Functional Package.

GUIDANCE FOR REVIEWERS

When providing feedback on this Functional Package, the author requests the reviewer to answer these questions:

(1) Is the reviewer able to clearly establish the traceability from a given "HCFA Internet Security Policy Requirement" to a "System Security Objective" to "System Security Requirement" in the document.

(2) Does the reviewer find the pre-defined ISO/IEC 15408 components used to express security requirements sufficiently clear and unambiguous ?

(3) Is the author confident that the set of operations (like Iteration, Assignment, Selection & Refinement) that are provided in ISO/IEC 15408 are comprehensive enough to express any security service requirement for any type of information system ?

(4) From an IT system vendor perspective – Has the security requirements expressed using ISO/IEC 15408 components in this Functional Package been stated at (a) correct level of granularity (b) too high a level or (c) too low a level ?

(5) From an IT system user/procurer perspective – Has the security requirements expressed using ISO/IEC 15408 components in this Functional Package been stated at (a) correct level of granularity (b) too high a level or (c) too low a level ?

(6) Do the reference to available standards in stating the security requirements in this Functional Package: (a) useful or (b) too restrictive ?

(7) Is the Functional Package overall an useful tool for translating the "policy requirements/threat model requirements" to "system-level security specifications" ? What aspects of this approach can be improved ?